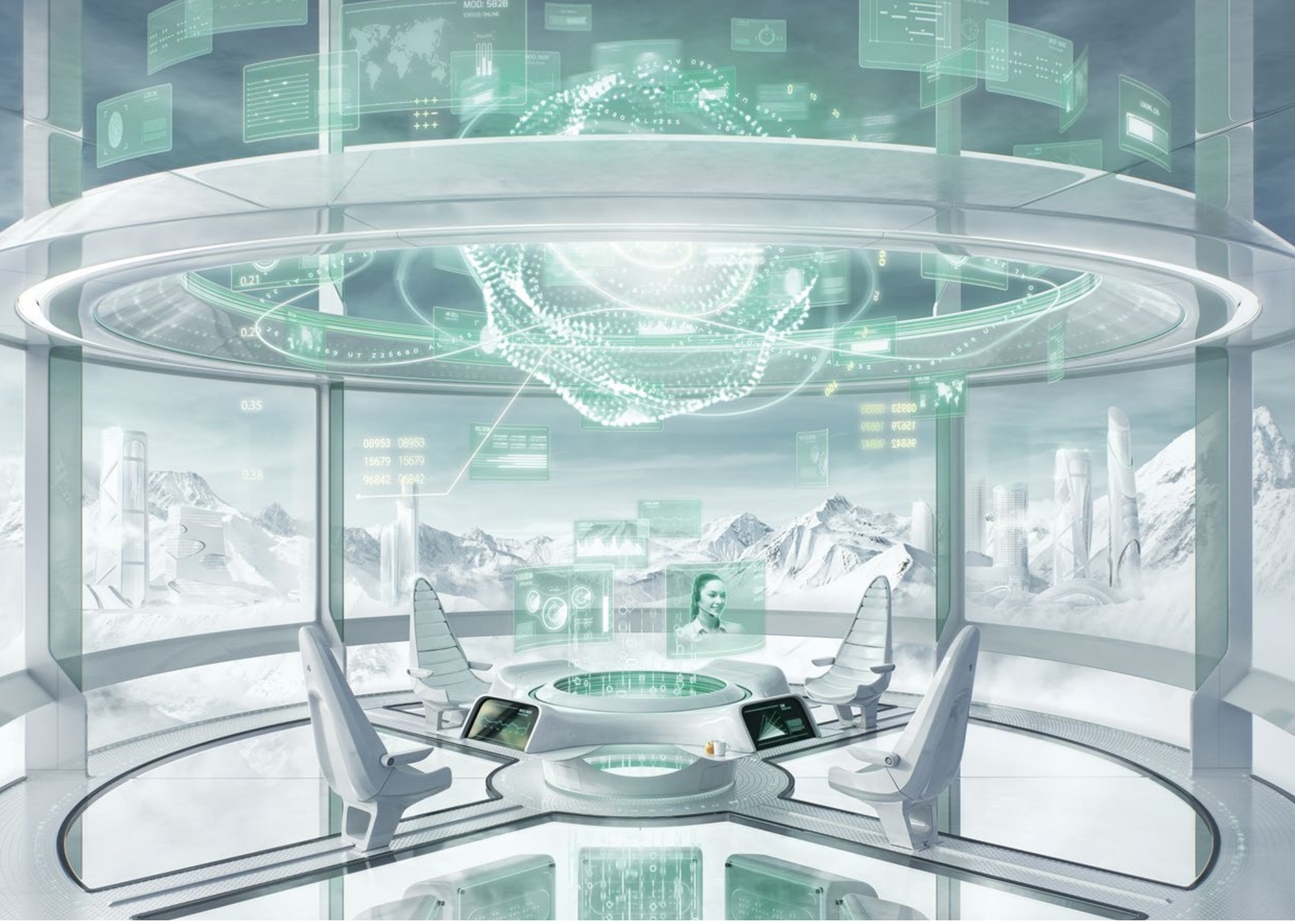


Effective training for employees. Ease of use for managers.

k-asap.com

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky BRING ON THE FUTURE

Kaspersky
Automated Security
Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

More than 80% of all cyber-incidents are caused by human error, with companies losing millions recovering from staff-related incidents. Yet the effectiveness of traditional training programs intended to prevent these problems is limited, and frequently fail to inspire and stimulate the necessary behavior.

Human mistakes as the biggest cyber-risk today

$1,195, 000
per enterprise organization
The average financial impact of data breaches caused by inappropriate IT resource use by employees*

$116,000
per SMB
The average financial impact of data breaches caused by inappropriate IT resource use by employees*

52%
of companies
regard employees as the biggest threat to corporate cybersecurity**

30%
of employees
admit that they share their work PC's login and password details with colleagues***

23%
of organizations
do not have any cybersecurity rules or policies in place for corporate data storage***

Barriers to launching an efficient security awareness program

While companies are eager to implement security awareness programs, many are unhappy with both the process and the results. Small and medium businesses, which don't usually have the experience and resources needed, are particularly challenged in this area.

Not efficient for students:

- Perceived as difficult, boring, irrelevant drudgery.
- It's all about 'don't' rather than about 'how to'
- Knowledge is not retained
- Reading and listening isn't as effective as doing

An administrative burden:

- How to create a program and set goals?
- How to manage training assignments?
- How to control the progress?
- How to fully engage people with the training?

* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky Lab, 2019

** Research: "The cost of a data breach", Kaspersky Lab, Spring 2018.

*** "Sorting out a Digital Clutter", Kaspersky Lab, 2019.

Efficiency and ease of awareness management for organizations of any size

Introducing the Automated Security Awareness Platform, which forms the core of the Kaspersky Security Awareness training portfolio.

The Platform is an online tool that builds strong, practical cyber-hygiene skills for employees throughout the year. Launching and managing the Platform doesn't require special resources or arrangements, and it provides the organization with built-in help at every step of the journey towards a safe corporate cyber-environment.

How to evaluate an awareness program

One of the most important criteria when choosing an awareness program is its efficiency. With ASAP, efficiency is built into the training content and management. The platform's content is based on a competency model consisting of 350 practical and essential cybersecurity skills that all employees should have. Without these skills, whether through ignorance or negligence, employees can harm the business.

Efficient training

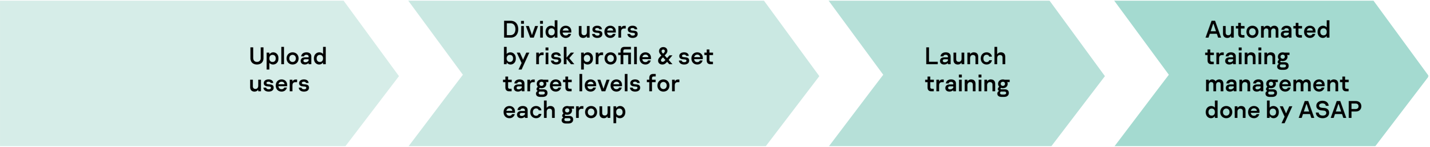
Consistent	– Well thought-out, structured content – Interactive lessons, constant reinforcement, tests, simulated phishing attacks to ensure skills will be applied Training materials and their structure are arranged in accordance with the specifics of human memory, our ability to absorb and retain information.
Practical & engaging	– Relevant to employees' everyday working life – Skills that can be put to immediate use Examples from real life situations in which employees can recognize themselves contribute to learner engagement while helping to retain information.
Positive	– Puts a proactive spin on safe behavior – Explains 'why' and 'how to' instead of the taboos Too many rules and restrictions can cause discontent, while explanations and convictions aligned with the way people think naturally contribute to adoption and behavior change.

Easy management

Easy to manage	Fully automated learning management brings every employee up to the security skills level appropriate to their risk profile without any intervention of the platform administrator
Easy to control	"All-in-one" dashboard & actionable reports
Easy to engage	Invitations and motivational emails as well as weekly student and administrators reports are sent automatically by the Platform.

ASAP management: simplicity through full automation

Start your program in 4 simple steps



Upload users

Divide users by risk profile & set target levels for each group

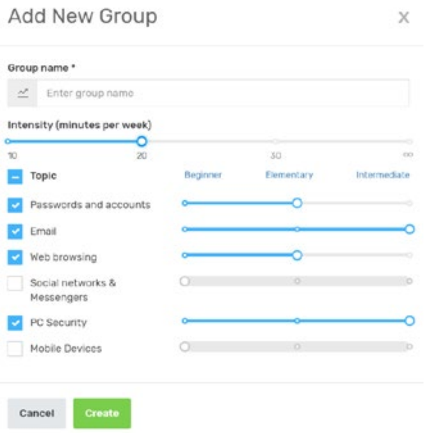
Launch training

Automated training management done by ASAP

This is the only step where the administrator needs to think and make decisions

The platform builds an education schedule for each group, based on pace and target level, and delivers actionable reporting and recommendations

Flexible learning path



Add New Group

Group name *

Enter group name

Intensity (minutes per week)

10 20 30 ∞

		Beginner	Elementary	Intermediate
☐	Topic			
☑	Passwords and accounts		●	
☑	Email			●
☑	Web browsing		●	
☐	Social networks & Messengers			
☑	PC Security			●
☐	Mobile Devices			

Adjusts to the individual pace and learning abilities of each employee

- The platform automatically ensures that users learn and pass tests on the basics before progressing to the next level
- No need for management to spend time on individual progress analysis and manual adjustments

Benefit from specific learning paths for each risk profile

Use automated rules to assign employees to a certain group based on their desired educational target level. This target level depends on the risk their particular role poses to the company. The higher the risk, the higher the target education level should be, e.g. IT or accountants typically represent a higher risk than other workers.

Flexible learning

- The scope of the training is completely flexible, while retaining the advantages of sequential automated learning management
- For each training group you are able to select:
  - Topics which students in the group need to learn (and skipping the ones that you don’t want to train now).
  - The target level you want students to achieve for each particular topic. Employees won’t spend their working time on learning irrelevant topics.

Get actionable reports anytime

- Enjoy dashboards with all the information needed to control
- Get suggestions on how to improve results
- Download reports from the main page in a single click, and configure the frequency of receiving reports by mail

ASAP methodology

Continuous incremental learning

- From the simple to the more complex, topic by topic and level by level: learning knowledge increases
- Expanding and applying previously acquired knowledge in new contexts

Multimodal content

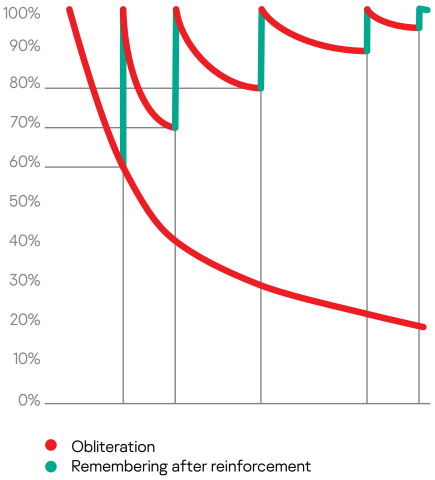
- Each level includes: Interactive lesson reinforcement assessment (test and simulated phishing attack where applicable)
- All training elements support the particular skill being taught in each unit, so that skills are truly mastered and become part of the new, desired behaviorInterval learning

Interval learning

- The Ebbinghaus 'forgetting curve' – learning methodology based on the specifics of human memory
- Repetition forms builds safe habits and prevents forgetting
- Reinforcement in each every module

The Ebbinghaus Forgetting curve

Repeated reinforcement helps build strong skills.



Training topics

Each topic comprises several levels, detailing specific security skills. Levels are defined according to degrees of risk they help eliminate: Level 1 is normally enough to protect from easiest and mass attacks while to protect from the most sophisticated and targeted attacks, one needs to study the next levels.

- Passwords & Accounts
- Email
- Web browsing
- Social networks & Messengers
- PC Security
- Mobile Devices
- Confidential data
- GDPR

Example: Skills trained in "Web browsing" topic

Beginner To avoid mass (cheap and easy) attacks	**Elementary** To avoid mass attacks on a specific profile	**Intermediate** To avoid well-prepared focused attacks	**Advanced*** To avoid targeted attacks
13 skills, including: – Set up your PC (updates, antivirus) – Ignore obviously malicious websites (those which ask to update software, optimize PC performance, send SMS, install players, etc.) – Never open executables from websites	**20 skills, including:** – Sign-up/Login with trusted sites only – Avoid numeric links – Enter sensitive information on trusted sites only – Recognize the signs of a malicious website	**14 skills, including:** – Recognize faked links – Recognize malicious files and downloads – Recognize malicious software	**13 skills, including:** – Recognize sophisticated fake links (including links looking like your company websites, links with redirects) – Avoid black-SEO sites – Log out when finished – Advanced PC setup (turn off Java, adblock, noscript, etc.)
	+ reinforcement of elementary skills	+ reinforcement of the previous skills	+ reinforcement of the previous skills

Key subjects covered in the topic: Links, Downloads, Software installations, Sign-up & Login, Payments, SSL

* Will be added during 2021

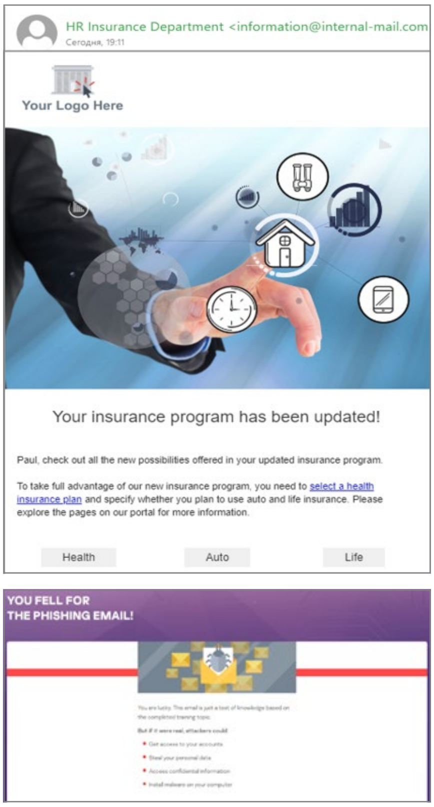
Languages

The Platform (both student's and admin interface) are available in the following languages:

- Arabic
- Dutch
- English
- French
- German
- Italian
- Portuguese
- Russian
- Spanish
- Czech
- Kazakh
- Polish
- Slovenian
- Rumanian
- Turkish
- Hungarian
- Danish
- Swedish
- Greek*
- Serbian
- Brazil (Portuguese)*

* are coming in Q1 2021

Example of the editable simulated phisihing template and the feedback



HR Insurance Department <information@internal-mail.com

Сегодня, 19:11

Your insurance program has been updated!

Paul, check out all the new possibilities offered in your updated insurance program.

To take full advantage of our new insurance program, you need to select a health insurance plan and specify whether you plan to use auto and life insurance. Please explore the pages on our portal for more information.

YOU FELL FOR THE PHISHING EMAIL!

You are lucky. This email is just a test of knowledge based on the completed training topic.

But if it were real, attackers could:

- Get access to your accounts
- Steal your personal data
- Access confidential information
- Install malware on your computer

Well-balanced, structured content and relevance to real life ensure efficiency

Learning principles in ASAP are based on the methodology that takes into account the specifics of human nature, our ability to perceive and absorb information. The content is full of real life examples and cases that highlight the personal importance of cybersecurity for employees.The Platform focuses on training skills, not just providing knowledge, so practical exercises and employee-related tasks are at the core of each module.

Modules combine different types of exercise to keep users interested and alert and to motivate them to learn and acquire safe behavior.

Visual style and texts are not only translated into different languages, but are adjusted to reflect different cultures and local attitudes.

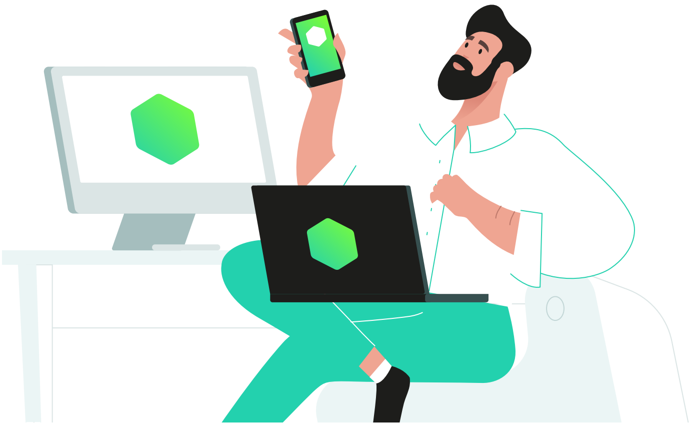
Simulation-based tasks and exercises to build practical skills and keep users entertained and motivated

Simulated phishing campaigns

Phishing campaigns are an addition to the main training process that test employees' practical skills avoiding phishing attacks. This will help the training manager identify gaps in user knowledge and encourage them to study topics they're having trouble with.

The platform comes with ready-made email templates containing phishing examples that can be sent to platform users in all available languages.The set of available templates is regularly updated with new ones. You can also create custom emails based on predefined templates.

Try a simulated phishing attack before you start the training - check your employees' resilience! It will help employees and management to see the benefits of training.



Kaspersky Security Awareness – a new approach to mastering IT security skills

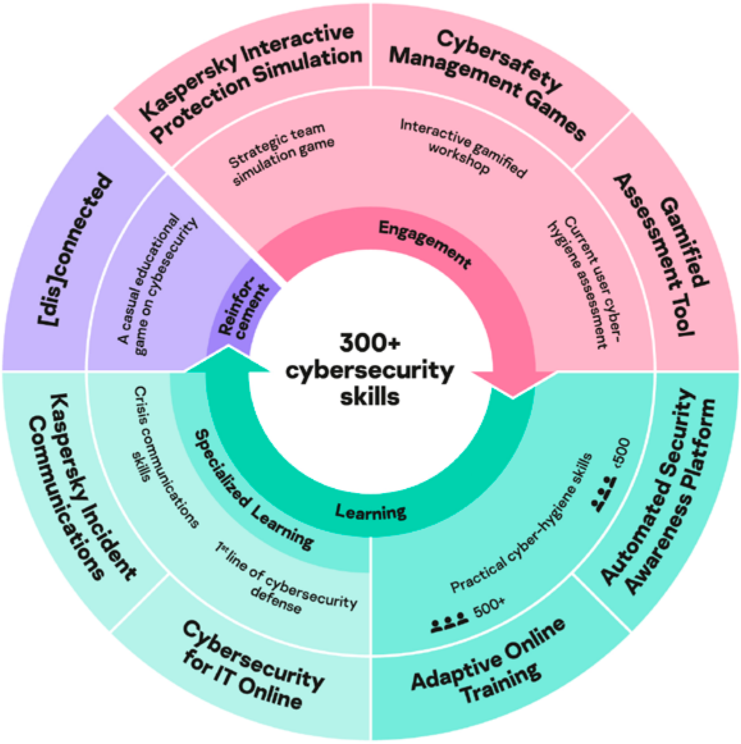
Key program differentiators

Substantial cybersecurity expertise
20+ years' experience in cybersecurity transformed into a cybersafety skillset that lies at the heart of our products

Training that change employees' behavior at every level of your organization
Our gamified training provides engagement and motivation through edutainment, while the learning platforms help to internalize the cybersecurity skillset to ensure that learnt skills don't get lost along the way.

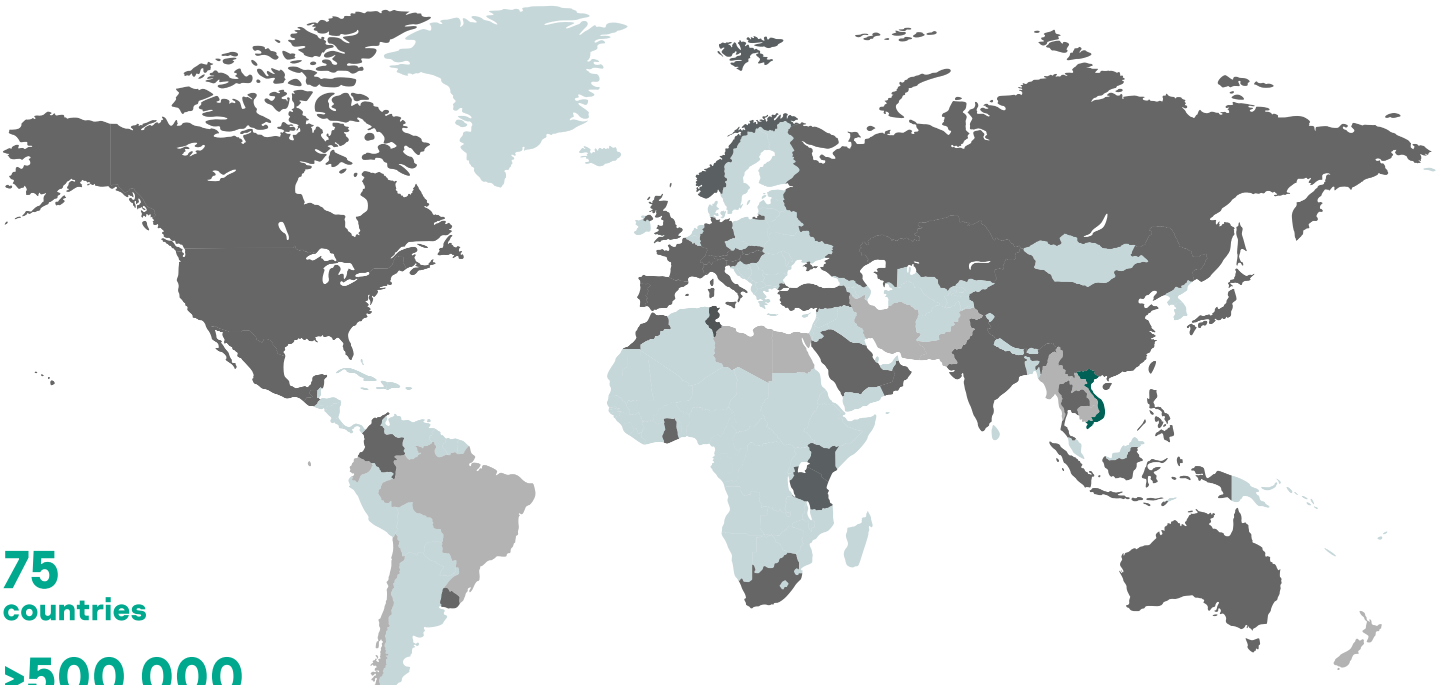
Kaspersky Security Awareness offers a range of highly engaging and effective training solutions that boost the cybersecurity awareness of your staff so that they all play their part in the overall cybersafety of your organization. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle that includes multiple components.

Different training formats for different organizational levels



Kaspersky Interactive Protection Simulation
Cybersafety Management Games
Gamified Assessment Tool
Automated Security Awareness Platform
Adaptive Online Training
Cybersecurity for IT Online
Kaspersky Incident Communications
[dis]connected
Strategic team simulation game
Interactive gamified workshop
Current user cyber-hygiene assessment
<500
Practical cyber-hygiene skills
500+
1st line of cybersecurity defense
Crisis communications skills
A casual educational game on cybersecurity
Engagement
Learning
Specialized Learning
Reinfor-cement
300+ cybersecurity skills

Kaspersky Security Awareness worldwide



75
countries

>500,000
trained employees

Kaspersky ASAP free trial: k-asap.com
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
IT Security News: business.kaspersky.com

www.kaspersky.com

kaspersky

**BRING ON
THE FUTURE**